PROCEDE DE DIVISION ENTIERE OU DE REDUCTION MODULAIRE SECURISE CONTRE LES ATTAQUES A CANAUX CACHES

L'invention concerne un procédé de division entière ou de réduction modulaire sécurisé contre les attaques à canal caché, et notamment les attaques différentielles. L'invention peut être utilisée pour réaliser des opérations de division dans un procédé cryptographique plus général, par exemple un procédé cryptographique à clé secrète ou publique. Un tel procédé cryptographique peut par exemple être mis en œuvre dans des dispositifs électroniques tels que des cartes à puce.

La sécurité des procédés cryptographiques réside dans leur capacité à maintenir cachées les données confidentielles ou des données dérivées des données confidentielles qu'ils manipulent.

Un utilisateur malveillant peut éventuellement engager des attaques, visant à découvrir notamment des données confidentielles contenues et manipulées dans des traitements effectués par le dispositif de calcul exécutant un procédé cryptographique.

Parmi les attaques les plus connues, on peut citer les attaques à canaux cachés, simples ou différentielles. On entend par attaque à canal caché une attaque basée sur une grandeur physique mesurable de l'extérieur du dispositif, et dont l'analyse directe (attaque simple) ou l'analyse selon une méthode statistique (attaque différentielle) permet de découvrir des données manipulées dans des traitements réalisés dans le dispositif. Ces attaques ont notamment été dévoilées par Paul Kocher (Advances in Cryptology - CRYPTO'99, vol. 1666 of Lecture Notes in Computer Science, pp.388-397. Springer-Verlag, 1999).

Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer le temps d'exécution, la consommation en courant, le champ électromagnétique rayonné par la partie du composant utilisée pour exécuter le calcul, etc. Au cours de l'exécution d'un procédé, la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, laisse une empreinte particulière sur la grandeur physique considérée, selon la valeur de ce bit et / ou selon l'instruction. Dit autrement, la trace (c'est-à-dire l'évolution dans le temps de la grandeur physique considérée) laissée par le composant exécutant le procédé est différente selon qu'on manipule un bit égal à 1 ou un bit égal à 0. Les attaques à canal caché sont basées sur cette faiblesse des procédés cryptographiques.

Les procédés cryptographiques utilisant comme opération de base une opération d'exponentiation modulaire de type $Y = X^D$, X, Y et D étant des nombres entiers ont été très largement étudiés ces dernières années. A titre d'exemple, on peut citer le procédé RSA, l'échange de clé selon Diffie-Hellman ou le procédé de signature DSA. Des progrès significatifs ont été réalisés pour protéger ces procédés contre les attaques à canaux cachés.

Par contre, certains procédés cryptographiques utilisent comme opération élémentaire une division entière de type q = a div b et / ou une réduction modulaire de type r = a mod b, a et b étant deux opérandes, q et r étant respectivement le quotient et le reste de la division entière de a par b. a et / ou b sont des données secrètes, par exemple des éléments d'une clé du procédé. Par exemple, le procédé de Barrett (P. Barret, "Implementing the RSA public key encryption algorithm on a standard digital signal processing", vol 263 of Lecture Notes in Computer Science, pp. 311-323,

Springer Verlag, 1987), le procédé de Quisquater (US patent 5,166,978, nov 92) ou le procédé RSA mis en œuvre selon le théorème des restes chinois (JJ Quisquater and C Couvreur, "Fast decipherment algorithm for RSA public key cryptosystem", Electronics Letters ., vol 18, pp. 905-907, Octobre 1982) sont des procédés cryptographiques utilisant une division entière comme opération élémentaire.

De tels procédés cryptographiques utilisant un procédé de division entière et / ou un procédé de réduction modulaire sont sensibles aux attaques à canal caché, comme on va le voir dans l'exemple ci-dessous.

Un procédé connu pour mettre en œuvre à la fois une division entière et une réduction modulaire est le procédé dit "papier crayon". Ce procédé reprend en pratique la méthode utilisée lorsqu'une telle opération est réalisée à la main. Ce procédé est rappelé ci-dessous.

Etant donné deux données a = $(a_{m-1}, \ldots, a_0)$ de m bits et b = $(b_{n-1}, \ldots, b_0)$ de n bits, n inférieur ou égal à m et b_{n-1} γ 0, le procédé de division dit "papier crayon" calcule le quotient q = a div b et le reste r = a div b. Pour cela, le procédé réalise successivement plusieurs divisions d'un entier A de n+1 bits par l'entier b de n bits. On doit avoir en pratique 0 [A/b < 2, ce qui est le cas chaque fois que b_{n-1} γ 0.

Le reste r est un nombre de au plus n bits puisque r < b. Le quotient q est quant à lui un nombre de au plus m-n+1 bits puisque q = a div b [a div $(b_{n-1}*2^{n-1})$ = a div 2^{n-1} = $(a_{m-1}, \ldots, a_{n-1})$ car b μ $b_{n-1}*2^{n-1}$ et $(a_{m-1}, \ldots, a_{n-1})$ est un nombre de m-n+1 bits. A la fin du procédé de division, le quotient q est mémorisé dans les m-n+1 bits de poids les plus faibles du registre contenant initialement le nombre a. Le bit de poids le plus fort du reste r est mémorisé dans un registre de 1 bit utilisé

comme retenue (carry) pendant le calcul et les n-1 bits de poids les plus faibles du reste r sont mémorisés dans les n-1 bits de poids les plus forts du registre contenant initialement le nombre a.

Comme on travaille en base 2, le bit de quotient de la division entière A div b a seulement deux valeurs possibles : 0 ou 1. Aussi une manière simple de réaliser l'opération A div b consiste à soustraire b à A puis à tester le résultat : si le résultat de A - b est positif, alors A div b = 1, si le résultat de A - b est strictement négatif, alors A div b = 0.

Le procédé de division complet peut alors s'écrire de la manière suivante :

Entrée : $a = (0, a_{m-1}, \ldots, a_0)$
$b = (b_{n-1}, \ldots, b_0)$
Sortie : $q = a \text{ div } b$ et $r = a \bmod b$
$A = (0, a_{m-1}, \ldots, a_{m-n+1})$
Pour $j = 1$ à $(m-n+1)$, faire :
$a \leftarrow SHL_{m+1}(a, 1)$; $\sigma \leftarrow$ carry
$A \leftarrow SUB_n(A, b)$; $\sigma \leftarrow \sigma$ OU carry
si $(\neg\sigma =$ VRAI) alors $A \leftarrow ADD_n(A, b)$
sinon $lsb(a) = 1$
Fin Pour

Procédé 1

Dans ce procédé, et dans tout ce qui suit, les notations suivantes sont utilisées.

Par abus de langage mais surtout par souci de clarté, et sauf précision explicite, on utilisera le même nom pour parler d'un registre et de son contenu. Ainsi on parlera du registre A pour parler du registre contenant la donnée A.

Le symbole "<-" et la notation y <- x sont utilisés pour indiquer le chargement du contenu du registre x dans un registre y dont le contenu est appelé également y.

A est un mot de n bits correspondant au contenu des n bits de poids les plus forts du registre contenant initialement la donnée a. Le registre A est bien sûr modifié à chaque itération, de même que le registre contenant initialement a.

σ indique si la soustraction a été effectuée à tort ou pas (ie si le bit de quotient doit être égal à 0 ou à 1).

$\neg\sigma$ est le complément à 1 (encore appelé négation) de la variable σ. VRAI est une constante, égale à 1 dans un exemple.

lsb(a) est le bit de poids le plus faible du nombre a, également appelé bit le moins significatif de a.

$SHL_{m+1}(a, 1)$ est une opération de décalage à gauche de 1 bit dans le registre de m+1 bits contenant la donnée a, le bit sortant du registre étant mémorisé dans la variable carry et un bit égal à 0 étant entré en bit de poids le plus faible du registre contenant initialement la donnée a.

$ADD_n(A, b)$ est une opération d'addition des n bits du nombre b aux n bits du mot A. On notera que l'opération $SHL_n(a, 1)$ est équivalente à l'opération $ADD_n(a, a)$. Bien sûr l'addition $ADD_n(A, b)$ est réalisée en additionnant, dans un circuit d'addition approprié, le contenu de deux registres contenant respectivement A et b.

$SUB_n(A, b)$ est une opération de soustraction du nombre b au mot A. Bien sûr la soustraction $SUB_n(A, b)$ est réalisée en soustrayant, dans un circuit approprié, le contenu d'un registre contenant la donnée b au contenu du registre contenant le mot A.

En résumé, le procédé 1 réalise les étapes suivantes :

- si $a <- SHL_{m+1}(a, 1)$ génère une retenue (σ = carry = 1), cela signifie que $a_m = 1$ (avant décalage) et donc que b doit être soustrait à A.

- si $a_m = 0$ (avant décalage) et si A <- $SUB_n(A, b)$ génère une retenue (carry = 1), cela signifie que A - b μ 0 avant la soustraction et donc b doit être soustrait à A.

- si a <- $SHL_{m+1}(a; 1)$ ne génère pas de retenue et si A <- $SUB_n(A, b)$ ne génère pas non plus de retenue (c'est-à-dire si, après mise à jour de σ, σ est FAUX (ou $\neg\sigma$ est VRAI, FAUX étant la négation de VRAI), alors cela signifie que A - b < 0 *avant* la soustraction et donc que b n'aurait pas dû être soustrait à A. Dans ce cas, le procédé réalise une opération d'addition A <- $ADD_n(A, b)$ pour restaurer la valeur de A.

Le procédé 1 est sensible aux attaques à canal caché. En effet, on remarque sur le procédé 1 que, à chaque itération, selon la valeur de σ, c'est-à-dire selon la valeur du bit de quotient qui sera obtenu lors de l'itération en cours, on effectue soit une addition $ADD_n(A, b)$ soit une mise à 1 du bit de poids le plus faible du registre contenant la donnée a. La mise en œuvre et la durée d'exécution de ces deux opérations sont différentes et la trace qu'elles laissent lors de leur mise en œuvre est également différente. La trace globale laissée au cours d'une itération varie donc en fonction du bit de résultat obtenu lors de ladite itération. En mesurant et en étudiant par exemple la trace laissée par le composant lors de l'exécution du procédé complet, par exemple dans le cadre d'une attaque différentielle, il est alors possible de déterminer bit à bit la valeur des bits de résultat.

Le procédé 1 permet d'obtenir à la fois le résultat de la division entière (q = a div b) et le reste de la division entière (r = a mod b) qui est aussi le résultat d'une réduction modulaire. D'autres procédés connus présentant les mêmes inconvénients réalisent soit une division modulaire seule, soit une réduction modulaire

seule. De manière générale, un procédé de division est assez similaire à un procédé de réduction modulaire.

Un but de l'invention est de sécuriser un procédé de mise en œuvre d'une division et / ou d'une réduction modulaire.

Dans ce but, l'invention propose un procédé cryptographique au cours duquel on réalise une division entière de type q = a div b et / ou une réduction modulaire de type r = a mod b, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort du nombre b.

Selon l'invention, le procédé est caractérisé en ce qu'on masque le nombre a par un nombre aléatoire ρ avant de réaliser la division entière et / ou la réduction modulaire.

Le nombre a étant masqué par un nombre aléatoire, la trace (par exemple la consommation énergétique) laissée lors de l'exécution du procédé est différente à chaque exécution, de sorte qu'il n'est plus possible de mettre en œuvre une attaque à canal caché différentielle.

L'invention peut être appliquée par exemple au procédé 1 qui réalise à la fois une division et une réduction modulaire. L'invention peut être plus généralement appliquée à tout procédé qui réalise l'une ou l'autre des ces opérations.

Le nombre aléatoire ρ peut être modifié à chaque exécution du procédé, ou bien simplement après un nombre prédéfini d'exécutions du procédé. Le cas échéant, le dit nombre prédéfini est choisi de préférence relativement petit, par exemple un nombre de 32 à 64 bits.

Selon un mode de réalisation préféré de l'invention, pour masquer le nombre a, on ajoute, au nombre a, b fois le nombre aléatoire (a <- a + b*ρ). Pour cela, concrètement, le contenu du registre b est

multiplié par le nombre aléatoire ρ puis additionné au nombre a et le résultat de l'addition est ensuite mémorisé dans le registre contenant initialement le nombre a.

Puis, on réalise ensuite la division entière et / ou la réduction modulaire souhaitée.

Dans le cas où une division entière est réalisée, le résultat de la division entière réalisée avec le nombre a masqué sous la forme a + b*ρ est égal à a div b + ρ. Dans ce cas, après la division entière, on enlève au résultat de la division entière la contribution apportée par le nombre aléatoire ρ pour retrouver le résultat attendu de la division entière sur le nombre a, c'est-à-dire a div b.

Dans le cas où réduction modulaire est réalisée, le résultat de l'opération (a + b*ρ) mod b est égal à a mod b, résultat attendu de la réduction modulaire sur le nombre a.

L'invention concerne également un composant électronique comprenant des moyens pour la mise en œuvre d'un procédé selon l'invention, tel que décrit ci-dessus. Les moyens de calcul programmés comprennent notamment plusieurs registres pour mémoriser les nombres a et b.

Enfin, l'invention concerne une carte à puce comprenant un composant ayant les caractéristiques décrites ci-dessus.

REVENDICATIONS

1. Procédé cryptographique au cours duquel on réalise une division entière de type q = a div b et / ou une réduction modulaire de type r = a mod b, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort du nombre b, caractérisé en ce qu'on masque le nombre a par un nombre aléatoire ρ avant de réaliser la division entière et / ou la réduction modulaire.

2. Procédé selon la revendication 1, au cours duquel, pour masquer le nombre a, on ajoute au nombre a, b fois le nombre aléatoire ρ (a <- a + b*ρ).

3. Procédé selon la revendication 1 ou la revendication 2, dans lequel, après avoir réalisé une division entière, on enlève au résultat de la division entière la contribution apportée par le nombre aléatoire ρ.

4. Procédé selon la revendication 3 en combinaison avec la revendication 2, au cours duquel, pour enlever la contribution apportée par le nombre aléatoire ρ, on soustrait le dit nombre aléatoire ρ au résultat de la division entière.

5. Procédé selon l'une des revendications 1 à 4, au cours duquel le nombre aléatoire ρ est modifié à chaque mise en œuvre du procédé.

6. Procédé selon l'une des revendications 1 à 4, au cours duquel le nombre aléatoire ρ est modifié après un nombre prédéterminé de mise en œuvre du procédé.

7. Composant électronique comprenant des moyens pour la mise en œuvre d'un procédé selon l'une des revendication précédente, les moyens de calcul programmés comprenant notamment plusieurs registres pour mémoriser les nombres a et b.

8. Carte à puce comprenant un composant selon la revendication précédente.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/[redacted]03/03681

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 199 63 407 A (GIESECKE & DEVRIENT GMBH) 12 July 2001 (2001-07-12) column 1, line 42 -column 3, line 53 ---	1-8
A	EP 0 682 327 A (YEDA RES & DEV) 15 November 1995 (1995-11-15) the whole document -----	1-8

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2004	- 5. MAI 2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/[redacted]03/03681

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19963407 A	12-07-2001	DE 19963407 A1	12-07-2001
		AU 3015101 A	09-07-2001
		CN 1415106 T	30-04-2003
		WO 0148706 A1	05-07-2001
		EP 1272984 A1	08-01-2003
		JP 2003525538 T	26-08-2003
		US 2003079139 A1	24-04-2003
EP 0682327 A	15-11-1995	US 5504817 A	02-04-1996
		EP 0682327 A2	15-11-1995
		IL 113662 A	06-12-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/[redacted] 03/03681

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	DE 199 63 407 A (GIESECKE & DEVRIENT GMBH) 12 juillet 2001 (2001-07-12) colonne 1, ligne 42 -colonne 3, ligne 53 ---	1-8
A	EP 0 682 327 A (YEDA RES & DEV) 15 novembre 1995 (1995-11-15) le document en entier -----	1-8

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
27 avril 2004	- 5. MAI 2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/[redacted]03/03681

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 19963407 A	12-07-2001	DE 19963407 A1	12-07-2001
		AU 3015101 A	09-07-2001
		CN 1415106 T	30-04-2003
		WO 0148706 A1	05-07-2001
		EP 1272984 A1	08-01-2003
		JP 2003525538 T	26-08-2003
		US 2003079139 A1	24-04-2003
EP 0682327 A	15-11-1995	US 5504817 A	02-04-1996
		EP 0682327 A2	15-11-1995
		IL 113662 A	06-12-2000